Amendments to the Claims:

Please amend claims 1, 13, and 20 as indicated in this listing of claims which will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended): A method for providing a cryptographic service utilizing a server on a network, comprising:

(a) identifying, by the server, a client utilizing the network;

(b) generating a tunnel on the network using a first key;

(c) receiving a second key at the server from the client utilizing the tunnel, wherein the second key is encrypted by the client using the first key, the second key being a private key of a key pair; ~~and~~

(d) receiving a performance specification for the cryptographic service; and

~~(d)~~(e) performing the cryptographic service at the server for the client, responsive to the performance specification, the server using the second key to perform the cryptographic service, whereby the server off-loads a computational burden associated with the cryptographic service from the client.

2. (Previously presented): A method as recited in claim 1, wherein the second key is encrypted by the client using the first key.

3. (Previously presented): A method as recited in claim 2, wherein the second key comprises at least one parameter for the cryptographic service performed by the server.

4. (Canceled)

5. (Previously presented): A method as recited in claim 1, wherein the cryptographic service includes modular exponentiation.

6. (Previously presented): A method as recited in claim 1, further comprising the step of transmitting cryptographic service results to the client.

7. (Previously presented): A method as recited in claim 6, further comprising: the step of encrypting the cryptographic service results utilizing the first key.

8. (Previously presented): A method as recited in claim 6, wherein the cryptographic service results are transmitted to a third party.

9. (Previously presented): A method as recited in claim 1, further comprising the step of charging a fee for the cryptographic service performed by the server.

10. (Original): A method as recited in claim 9, wherein the fee is charged to the client.

11. (Original): A method as recited in claim 1, wherein the first key comprises an encryption key for a symmetric cipher.

12. (Original): A method as recited in claim 1, wherein the first key comprises an encryption key for an asymmetric cipher.

13. (Currently amended): A computer program embodied on a computer readable medium for providing a cryptographic service utilizing a server on a network, comprising:

(a) a code segment for identifying, by the server, a client utilizing the network;

(b) a code segment for generating a tunnel on the network using a first key;

(c) a code segment for receiving a second key at the server from the client utilizing the tunnel, wherein the second key is encrypted by the client using the first key, the second key being a private key of a key pair; ~~and~~

(d) a code segment for receiving a performance specification for the cryptographic service; and

~~(d)~~(e) a code segment for performing the cryptographic service at the server for the client, responsive to the performance specification, the server using the second key to perform the cryptographic service, whereby the server off-loads a computational burden associated with the cryptographic service from the client.

14. (Previously presented): A computer program as recited in claim 13, wherein the second key is encrypted by the client using the first key, and further comprising a code segment for receiving the second key at the server.

15. (Previously presented): A computer program as recited in claim 14, wherein the second key comprises at least one parameter for the cryptographic service performed by the server.

16. (Canceled):

17. (Previously presented): A computer program as recited in claim 13, wherein the cryptographic service includes modular exponentiation.

18. (Previously presented): A computer program as recited in claim 13, further comprising a code segment that transmits the cryptographic service results to the client.

19. (Previously presented): A computer program as recited in claim 18, further comprising a code segment that encrypts the cryptographic service results utilizing the first key.

20. (Currently amended): A system for providing a cryptographic service utilizing a server on a network, comprising:

(a) logic for identifying, by the server, a client utilizing the network;

(b) logic for generating a tunnel on the network using a first key;

(c) logic for receiving a second key at the server from the client utilizing the tunnel, wherein the second key is encrypted by the client using the first key, the second key being a private key of a key pair; ~~and~~

(d) logic for receiving a performance specification for the cryptographic service; and

~~(d)~~(e) logic for performing the cryptographic service at the server for the client, responsive to the performance specification, the server using the second key to

perform the cryptographic service, whereby the server off-loads a computational burden associated with the cryptographic service from the client.

21. (Previously presented): A method as recited in claim 3, wherein a message or a cyphertext comprises a second parameter for the cryptographic service performed by the server.

22. (Original): A method as recited in claim 21, wherein the message or cyphertext has been blinded by the user before transmittal to the server.